1   REBEKAH KAUFMAN (CA SBN 213222)
    RKaufman@mofo.com
2   ROBERT T. PETRAGLIA (CA SBN 264849)
    RPetraglia@mofo.com
3   MORRISON & FOERSTER LLP
    425 Market Street
4   San Francisco, California 94105-2482
    Telephone: 415.268.7000
5   Facsimile: 415.268.7522

6   MARC J. ZWILLINGER (*pro hac vice*)
    Marc@zwillgen.com
7   JACOB SOMMER (*pro hac vice*)
    Jake@zwillgen.com
8   ZWILLGEN PPLC
    1705 N. Street, NW
9   Washington, D.C. 20036
    Telephone: 202.706.5202
10 Facsimile: 202.706.5298

11 Attorneys for Defendant
    YAHOO! INC.

12

13   UNITED STATES DISTRICT COURT

14   NORTHERN DISTRICT OF CALIFORNIA

15   SAN JOSE DIVISION

16

17 CARSON PENKAVA, individually and on behalf of those similarly situated,	Case No. CV12-03414 PSG LHK
18	**YAHOO! INC.'S NOTICE OF MOTION**
19 Plaintiff,	**AND MOTION TO DISMISS OR, IN THE ALTERNATIVE, STRIKE CLASS ACTION ALLEGATIONS IN FIRST**
20 v.	**AMENDED COMPLAINT; MEMORANDUM OF POINTS AND**
21 YAHOO!, INC.,	**AUTHORITIES IN SUPPORT THEREOF**
22 Defendant.	**CLASS ACTION**
23	**HEARING:**
24	Date: March 21, 2013 Time: 1:30 p.m.
25	Place: Courtroom 4 Judge: The Honorable Lucy H. Koh
26	

27

28

DEFENDANT YAHOO! INC.'S NOTICE OF MOTION AND MOTION TO DISMISS OR STRIKE; MPA IN SUPPORT THEREOF
CASE NO. CV12-03414 PSG LHK
sf-3206847

1

NOTICE OF MOTION AND MOTION TO DISMISS OR, ALTERNATIVELY, STRIKE

2

TO PLAINTIFF AND HIS ATTORNEYS OF RECORD:

3

PLEASE TAKE NOTICE THAT on March 21, 2013, at 1:30 p.m., or as soon thereafter as

4

the matter may be heard, in the Courtroom of the Honorable Lucy H. Koh, located at the Robert

5

F. Peckham Federal Building, 280 South First Street, Fifth Floor, San Jose, California, Defendant

6

Yahoo! Inc. ("Yahoo!") will, and hereby does, move the Court for an order dismissing Plaintiff's

7

First Amended Complaint pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure or, in

8

the alternative, an order striking Plaintiff's class action allegations pursuant to Rule 12(f) of the

9

Federal Rules of Civil Procedure. This motion is based on the Notice of Motion and Motion, the

10

accompanying Memorandum of Points and Authorities, the accompanying Request for Judicial

11

Notice, the papers and records on file in this action, and such other written and oral argument as

12

may be presented to the Court.

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1

TABLE OF CONTENTS

2

Page

22

23

24

25

26

27

28

TABLE OF AUTHORITIES

Page(s)

CASES

MEMORANDUM OF POINTS AND AUTHORITIES

Defendant Yahoo! Inc. ("Yahoo!") respectfully submits this brief in support of its motion to dismiss the First Amended Complaint ("FAC") filed by Plaintiff Carson Penkava ("Plaintiff"), or, in the alternative, to strike the class action allegations set forth therein.

INTRODUCTION

Plaintiff brings this putative class action against Yahoo! for an alleged violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630 *et seq.*, based on Yahoo!'s purported interception, reading and recording of emails that Plaintiff, a non-Yahoo! email subscriber, sent to individual Yahoo! subscribers. This is Plaintiff's second attempt to state a claim. The FAC was filed in response to Yahoo!'s prior motion to dismiss, which identified the constitutional infirmities of Plaintiff's CIPA claim and the Complaint's failure to plead facts demonstrating a CIPA violation. The FAC, however, does nothing to overcome those deficiencies. Plaintiff instead merely attempts to conceal them by deleting the allegation that Yahoo! obtains consent from its users to scan and record emails prior to delivery, removing the admission that he continues to send emails to Yahoo! users even though he believes his emails are scanned and recorded by Yahoo!, and introducing the colorful phrase "creeping and peeping" to describe the routine, innocuous scanning and review of emails that is in fact the subject of the FAC. None of these revisions are sufficient to save Plaintiff's CIPA claim. In fact, Plaintiff's new, bad faith allegations may give rise to sanctions under Rule 11.

The CIPA is a state statute governing unauthorized "wiretaps" and "eavesdropping" of "confidential" communications without the "consent" of all parties. Nowhere do its provisions purport to apply to email communications, much less the routine scanning and access of emails in which providers of electronic communications services ("ECS Providers"), like Yahoo!, necessarily must engage to provide email services to their users. Indeed, Congress has enacted legislation, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 *et seq.*, that comprehensively regulates how ECS Providers may use, store and access such communications. In doing so, Congress intended ECPA to preempt any parallel state legislation, especially here where application of both the CIPA and ECPA would subject Yahoo! to criminal

DEFENDANT YAHOO! INC.'S NOTICE OF MOTION AND MOTION TO DISMISS; MPA IN SUPPORT THEREOF
CASE NO. CV12-03414 PSG LHK
sf-3206847

1

1   penalties and conflicting regulations in its <u>nationwide</u> provision of email services to its users.

2   Dismissal is proper on these grounds alone.

3   Plaintiff's CIPA claim also violates the Dormant Commerce Clause. Plaintiff alleges that

4   he is an <u>Alabama</u> resident who sent emails to Yahoo! subscribers, and he purports to represent a

5   class of individuals residing <u>outside of California</u> who sent emails to Yahoo! subscribers.

6   Plaintiff thus improperly seeks to regulate—through a <u>California</u> criminal statute—Yahoo!'s

7   handling of out-of-state emails sent by out-of-state residents, in direct contravention of the

8   Commerce Clause's prohibition against state law regulation of commerce taking place outside the

9   state's borders.

10   The Due Process and Full Faith and Credit Clauses of the United States Constitution are

11   violated for similar reasons. The Supreme Court has repeatedly held that the Constitution

12   restricts a state's power to apply its laws <u>beyond its borders</u>, and that a state must have significant

13   contacts to the claims asserted by <u>each</u> member of a putative class before its laws may

14   constitutionally be applied. *See*, *e.g.*, *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797 (1985).

15   Here, however, the CIPA would be applied to emails that were both sent and received in other

16   states, as the class as pled is composed only of individuals that reside and sent emails outside of

17   California.

18   California's long-standing presumption against extraterritorial application of its criminal

19   laws also prevents Plaintiff, a non-California resident, from applying the CIPA to conduct taking

20   place outside of California with respect to other non-California residents. *See Sullivan v. Oracle*

21   *Corp.*, 51 Cal. 4th 1191, 1207 (2011) ("we presume the Legislature did not intend a statute to be

22   operative, with respect to occurrences outside the state") (quotations and citation omitted).

23   Even if Plaintiff could constitutionally assert his CIPA claim, the FAC fails to state a

24   claim. The FAC contains only conclusory allegations to the effect that Yahoo! "reads, learns of

25   the content or meaning of, copies, records, and/or eavesdrops upon the communications sent by

26   Plaintiff and Class Members. " (FAC ¶ 37.) Absent are any requisite specific facts demonstrating

27   that the conduct at issue is anything other than the access and review in which an ECS Provider

28   must necessarily engage to deliver emails to the intended recipients and otherwise provide email

communication services to its subscribers. Also absent are specific allegations demonstrating the

plausibility of Plaintiff's conclusory assertions that his emails are "confidential" and that no party

gave "consent" to Yahoo!'s alleged scanning of emails.

Finally, a class consisting of the residents of 49 states and the District of Columbia (all but

California residents) cannot satisfy the requirements of Rule 23 of the Federal Rules of Civil

Procedure. Not only would multiple state laws need to be applied, thereby precluding Plaintiff

from establishing a predominance of common issues of law, but also many individual factual

issues would need to be determined before considering whether any given class member would be

entitled to relief, similarly precluding Plaintiff from establishing a predominance of common

issues of fact. The class action allegations must accordingly be stricken under Rule 12(f).

Plaintiff's CIPA claim is deficient as a matter of law, and amendment will not cure those

defects. Yahoo! accordingly respectfully requests that the Court dismiss the Complaint with

prejudice. Alternatively, the class action allegations should be stricken for failure to satisfy

Rule 23 of the Federal Rules of Civil Procedure.

ISSUES TO BE DECIDED

Whether applying the CIPA to Yahoo! is a violation of the Supremacy Clause of the

United States Constitution when Congress has preempted the field of regulation governing ECS

Providers' interception, use and disclosure of electronic communications.

Whether it is a violation of the Supremacy Clause of the United States Constitution to

apply the CIPA to Yahoo! when such application would conflict with federal regulations

governing how ECS Providers may access and use electronic communications.

Whether it is a violation of the Commerce Clause of the United States Constitution to

apply CIPA to regulate Yahoo!'s alleged treatment of out-of-state emails sent by out-of-state

residents when such application would constitute direct regulation of interstate commerce and

conflict with the laws of other states.

Whether it is a violation of the Due Process and Full Faith and Credit Clauses of the

United States Constitution and California's own presumption against extraterritorial application

of its laws to apply the CIPA to regulate Yahoo!'s alleged treatment of out-of-state emails sent by

1   out-of-state residents.

2   Whether Plaintiff's pleading of his CIPA claim is sufficient to state a claim regarding

3   wiretapping or eavesdropping of email communications.

4   Whether the class as defined could ever be certified under Rule 23 of the Federal Rules of

5   Civil Procedure.

6   **STATEMENT OF FACTS[1]**

7   The FAC asserts claims under Sections 631 and 632 of the CIPA. Section 631 of the

8   CIPA prohibits wiretaps or other unauthorized connections with any "telegraph or telephone wire,

9   line, cable, or instrument" and willfully reading or attempting to learn the contents or meaning of

10 any communication that is in transit "over any wire, line or cable" without the consent of all

11 parties to the communication. Cal. Penal Code § 631. Section 632 prohibits eavesdropping by

12 means of any "electronic amplifying or recording device" of any confidential communication

13 without the consent of all parties to the communication. Cal. Penal Code § 632. Plaintiff

14 contends that Yahoo! has violated § 631 by "scanning, processing, or copying" his emails while

15 they are in transit to Yahoo! Mail recipients (FAC ¶¶ 64-67); and that Yahoo! has violated § 632

16 by eavesdropping or recording his emails (*Id*. ¶ 69). Missing from the FAC, however, are a host

17 of requisite allegations demonstrating that the conduct at issue gives rise to a CIPA violation.

18   Plaintiff alleges that Yahoo! operates a web-based email service known as "Yahoo! Mail,"

19 that he does not have a personal Yahoo! email account, and that he has sent emails to unidentified

20 "Yahoo! Mail recipients." (*Id*. ¶¶ 16, 17, 19.) The crux of the FAC is Plaintiff's allegation,

21 restated in a variety of ways, that Yahoo! reads, records and eavesdrops on the emails Plaintiff

22 sends to Yahoo! Mail users. (*Id*. ¶¶ 32, 34, 64, 66, 69.) Plaintiff fails to allege facts, however,

23 that would demonstrate that Yahoo!'s conduct is anything more than the scanning that is

24 necessary for an ECS Provider to provide email services to its subscribers.

25   Further, Plaintiff merely pleads in a conclusory fashion that his emails are "confidential"

26 under § 632 (*id*. ¶ 71), but provides no factual support for that contention. Plaintiff fails to allege

27 _____

28 [1] Plaintiff's allegations, and Yahoo!'s descriptions herein, are necessarily limited to practices in the United States only.

DEFENDANT YAHOO! INC.'S NOTICE OF MOTION AND MOTION TO DISMISS OR STRIKE; MPA IN SUPPORT THEREOF   4
CASE NO. CV12- 03414 PSG LHK
sf-3206847

1   any facts demonstrating that he believed that the recipient of his emails would not forward, share

2   or otherwise publicize his emails, or that the emails were otherwise confidential.

3   Plaintiff also fails to allege any facts supporting his conclusory allegation that no party to

4   any emails sent by Plaintiff or any member of the putative class "consented" to Yahoo!'s alleged

5   scanning and recording of emails. (FAC ¶ 41.) In fact, the only two factual allegations that have

6   been pled regarding "consent" are <u>inconsistent</u> with the legal conclusion that no party gave their

7   consent. In particular, **Plaintiff alleged in his original Complaint that he believed Yahoo!**

8   **obtained consent from its subscribers to scan their emails.** (Original Compl. ¶ 3.) He also

9   alleged that he <u>continued</u> to email Yahoo! subscribers even after he came to believe that his

10 emails would be scanned and recorded (Original Compl. ¶ 11), and thus implicitly consented to

11 the scanning and recording of those emails. Those prior allegations demonstrate the

12 implausibility of Plaintiff's legal contention that no party gave their consent. *See Cole v.*

13 *Sunnyvale*, No. C-08-05017 RMW, 2010 U.S. Dist. LEXIS 11105, at *9-11 (N.D. Cal Feb. 9,

14 2010) ("The court may also consider the prior allegations [in the original complaint] as part of its

15 'context-specific' inquiry based on its judicial experience and common sense to assess whether

16 the [] Amended Complaint plausibly suggests an entitlement to relief, as required under *Iqbal*.").

17   **LEGAL STANDARD**

18   Under Federal Rule of Civil Procedure 12(b)(6), a complaint must be dismissed for failure

19 to state a claim if the plaintiff either fails to state a cognizable legal theory or has not alleged

20 sufficient facts to support a cognizable legal theory. *See* Fed. R. Civ. P. 12(b)(6); *Balistreri v.*

21 *Pacific Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990), *rev'd in part on other grounds by Bell*

22 *Atl. Corp. v. Twombly*, 550 U.S. 544, 562-63 (2007). A pleading that offers "labels and

23 conclusions" or "a formulaic recitation of the elements of a cause of action will not do."

24 *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotations and citation omitted). The complaint

25 must allege facts which, when taken as true, raise more than a speculative right to relief.

26 *Twombly*, 550 U.S. at 555. A court may also consider allegations in a prior complaint as part of

27 its context-specific inquiry to assess whether an amended complaint plausibly suggests an

28 entitlement to relief. *See Cole*, 2010 U.S. Dist. LEXIS 11105, at *9-11; *Fasugbe v. Willms*, No.

1   CIV 2:10-2320 WBS KJN, 2011 U.S. Dist. LEXIS 56569, at *13-16 (E.D. Cal. May 25, 2011).

2   Pursuant to Federal Rule of Civil Procedure 12(f), a party may move to strike from a

3   pleading "an insufficient defense or any redundant, immaterial, impertinent, or scandalous

4   matter." Fed. R. Civ. P. 12(f). "Where the complaint demonstrates that a class action cannot be

5   maintained on the facts alleged, a defendant may move to strike class allegations prior to

6   discovery." *Sanders v. Apple, Inc.*, 672 F. Supp. 2d 978, 990 (N.D. Cal. 2009). Further, under

7   Rule 23(c)(1), a court is fully empowered to determine "at an early practicable time" whether an

8   action is to be maintained as a class action. *Id.* at 990. Additionally, Rule 23(d) expressly

9   authorizes a court to issue orders requiring that the pleadings be amended to eliminate therefrom

10   allegations as to representation of absent persons, and that the action proceed accordingly. *Id.*

11   Consistent with these rules, motions to strike are a well-recognized means of attacking inadequate

12   class allegations such as those found here.

ARGUMENT

13

14   **I.   THE COMPLAINT MUST BE DISMISSED PURSUANT TO RULE 12(B)(6).**

15   **A.   ECPA Preempts Plaintiff's CIPA Claim.**

16   Plaintiff's CIPA claim must be dismissed because, to the extent the CIPA can properly be

17   interpreted to cover electronic communications, it is preempted by the Electronic

18   Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510 *et seq.*[2] In enacting ECPA, Congress

19   established a comprehensive privacy scheme governing how providers, such as Yahoo!, can

20   provide electronic communications services to their users. *See generally Bunnell v. Motion*

21   *Pictures Ass'n of Am.*, 567 F. Supp. 2d 1148, 1152, 1154 (C.D. Cal. 2006) ("The scheme of the

22   ECPA is very comprehensive: it regulates private parties' conduct, law enforcement conduct,

23   outlines a scheme covering both types of conduct and also includes a private right of action for

24   violation of the statute."). That "comprehensive" scheme completely occupies the field with

25

26   [2] "Pre-emption may be either expressed or implied," and "is compelled whether Congress'
     command is explicitly stated in the statute's language or implicitly contained in its structure and
27   purpose." *Gade v. Nat'l Solid Wastes Mgmt. Ass'n*, 505 U.S. 88, 98 (1992) (quotations and
     citation omitted). Absent explicit preemptive language, the Supreme Court has recognized at
28   least two types of implied preemption: field preemption and conflict preemption. *Id.*

regard to the use and disclosure of electronic communications and leaves no room for

"supplementary state regulation." *Id.* ECPA preempts Plaintiff's CIPA claim in two independent

ways: (1) field preemption and (2) conflict preemption.

> **1.** **ECPA Preempts the Field of State Laws Regulating Access, Use and Disclosure of Electronic Communications by ECS Providers.**

The comprehensive duties, responsibilities and rights of ECS Providers are established by

federal law and leave no room for additional state regulation. "[F]ield preemption" exists when

"Congress's intent to supersede state law altogether may be found from a scheme of federal

regulation so pervasive as to make reasonable the inference that Congress left no room for the

States to supplement it." *Sherwood Partners, Inc. v. Lycos, Inc.*, 394 F.3d 1198, 1200 (9th Cir.

2005) (quotations and citation omitted). In enacting ECPA, Congress intended that regulatory

scheme to supersede application of any state laws that would govern an ECS Provider's provision

of electronic communications services to its users.

ECPA is composed of two major components. *Bunnell*, 567 F. Supp. 2d at 1152. The

first is the Wiretap Act, under Title I of ECPA, which governs communications while in transit

and makes it an offense to "intentionally intercept[] . . . any wire, oral, or electronic

communication." *Id.* (citing 18 U.S.C. § 2511(1)(a).) The second is the Stored Communications

Act ("SCA"), under Title II of ECPA, which governs access to communications in electronic

storage and makes it an offense to improperly access stored electronic communications, except

for access by ECS Providers or access authorized by ECS users. 18 U.S.C. § 2701.

Titles I and II of ECPA together constitute an expansive regulatory scheme regarding how

internet service providers ("ISPs") may conduct business generally, and more specifically, when

ECS Providers may and may not access electronic communications—the very conduct at issue in

the Complaint. For instance, under ECPA, a provider of wire and electronic communications

may intercept communications while in transit for its own purposes (18 U.S.C. § 2511(2)(a)); on

law enforcement's behalf with the consent of one party (18 U.S.C. § 2511(2)(c)); for any

purposes with a party's consent (18 U.S.C. § 2511(2)(d)); on law enforcement's behalf pursuant

to legal process (18 U.S.C. § 2511(2)(b), (e), (f), (h), (i) & § 2518); or to intercept "public"

1   communications (18 U.S.C. § 2511(2)(g)). ECPA likewise provides specific rules for ISPs

2   regarding the disclosure of communications being transmitted through their services. 18 U.S.C.

3   § 2511(3)(a). Section 2511(3)(b) provides for disclosure as authorized under § 2511(2)(a); to law

4   enforcement as authorized under 18 U.S.C. § 2517; with the consent of one party (18 U.S.C.

5   § 2511(3)(b)(ii)); to forward communications (18 U.S.C. § 2511(3)(b)(iii)); or when inadvertently

6   obtained and involved in the commission of a crime (18 U.S.C. § 2511(3)(b)(iv)). ECPA even

7   provides enforcement mechanisms for the Communications Assistance for Law Enforcement Act

8   (47 U.S.C. §§ 1001, *et seq.*), which requires providers to maintain certain equipment to assist law

9   enforcement in intercepting communications.[3] 18 U.S.C. § 2522.

10   Likewise, ECPA regulates how ECS Providers may handle communications stored on

11 their servers. *See* 18 U.S.C. § 2701(a)(1). For example, the SCA provides rules for when ECS

12 Providers may and may not disclose stored communications (18 U.S.C. § 2702); and when they

13 *must* disclose communications.[4] 18 U.S.C. § 2703. The SCA also provides rules regarding when

14 providers may be compelled to preserve copies of communications (18 U.S.C. § 2704) and

15 provide counterintelligence agencies access to certain records (18 U.S.C. § 2709). Finally, the

16 SCA provides a private right of action when a service provider, a subscriber or another person

17 violates its unique provisions. 18 U.S.C. § 2707(a). The Court of Appeals for the Ninth Circuit

18 has specifically acknowledged that the SCA was created "for the express purpose of addressing

19 'access to stored . . . electronic communications and transactional records.'" *Konop v. Hawaiian*

20 *Airlines, Inc.*, 302 F.3d 868, 879 (9th Cir. 2002) (citing S. Rep. No. 99-541 at 3 (1986)).

21   ECPA's legislative history further demonstrates that Congress recognized the need for

22

23
    _____

24 [3] Congress also has provided rules regarding what offenses—even under state law—are sufficient
    to support an interception order (18 U.S.C. § 2516(2)), demanding that state orders comply with
    18 U.S.C. § 2518, and requiring that state courts must suppress evidence obtained in violation of
25 federal law (18 U.S.C. § 2515).

26 [4] Many of these rules also apply to providers of Remote Computing Services ("RCS"). Yahoo! is
    both an ECS and an RCS, depending on the service it provides. For purposes of this lawsuit,
    however, only Yahoo!'s electronic communications services are at issue. *See, e.g.*, *Hall v.*
27 *Earthlink Network, Inc.*, 396 F.3d 500, 502 (2d Cir. 2005) (Earthlink, providing email service,
    was ECS); *FTC v. Netscape Commc'ns Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000) (provider of
28 email accounts is an ECS).

uniform federal regulation of electronic communication service providers—which would not allow for the application of additional, much less contradictory, state law. In enacting ECPA, Congress recognized that, as part of providing electronic communication services, such as email, "the providers of electronic mail create electronic copies of private correspondence for later reference," and that "[t]his information is processed for the benefit of the user." (Request for Judicial Notice ("RJN") Ex. A at 3.) Because this information is under the service provider's control, the "information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties." *Id.* Congress concluded that "providers of these services can do little under current law to resist unauthorized access to communications." *Id.* Thus, Congress intended to protect users' privacy from misuse by law enforcement or unauthorized third parties, and to give providers definitive rules regarding what they can and cannot do as they process electronic communications for the benefit of their users nationwide.

Congress intended to allow "the employees of providers of wire or electronic communication services to intercept, disclose or use customer communications in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the provider, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks." (RJN Ex. A at 20.) Congress explained that:

> In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited.

Id. Congress thus carved out special exceptions to the general prohibitions on interception for monitoring of electronic communications. Congress's intent was that providers comply with ECPA, and no other set of laws, lest the delicate balance struck between the functional needs of

1 providers and law enforcement, and the privacy rights of users, be disrupted.

2 ECPA's comprehensive scheme thus completely preempts any parallel state legislation

3 that attempts to govern the conduct of ECS Providers. Congress's intent was that states not be

4 permitted to strike a different balance between users' privacy and the provision of electronic

5 communications services nationwide to their users. Indeed, this is precisely why the CIPA should

6 not be applied to the handling of electronic communications services. This case does not present

7 the question whether a state can require both parties to a wire or telephonic communication to

8 consent to the tapping or recording of that communication. This case is about whether a state can

9 apply its wiretapping and telephonic interception laws in a manner inconsistent with federal law;

10 requiring the senders of emails to give their consent before ECS Providers can filter, scan,

11 deliver, record and sort their users' email. ECPA preempts any such application of state law.

12 Finally, though federal courts in California have split over whether ECPA preempts the

13 CIPA, none of those cases considered the unique issue here—whether ECPA preempts parallel

14 state legislation regulating the conduct of email providers when providing nationwide electronic

15 communications services. *Compare In re Google Inc. Street View Elec. Commc'ns Litig.*, 794

16 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011) (holding that ECPA preempts the CIPA); *Bunnell*,

17 567 F. Supp. 2d at 1154 (same), *with Shively v. Carrier IQ, Inc.*, No. C-12-0290 EMC, 2012 U.S.

18 Dist. LEXIS 103237 (N.D. Cal. July 24, 2012) (holding that ECPA does not preempt the CIPA);

19 *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal 2011) (same). Generally, these cases

20 did not consider the SCA's provisions regarding electronic communications services. *See*

21 *generally id.* When confronted specifically with whether the SCA preempted California invasion

22 of privacy claims against a provider of text messaging services for disclosing those messages, the

23 District Court for the Central District of California held that California law was preempted.

24 *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1137-38 (C.D. Cal. 2006), *aff'd in*

25 *part and rev'd in part on other grounds by* 529 F.3d 892 (9th Cir. 2008).

26 **2.   The CIPA As Applied by Plaintiff Impermissibly Conflicts with ECPA.**

27 Even if ECPA did not preempt Plaintiff's CIPA claim on grounds of field preemption,

28 Plaintiff's claim nevertheless would be preempted because it directly conflicts with the provisions

1   of ECPA that allow ECS Providers to access email stored on their servers for various purposes

2   prior to the delivery of such mail to the recipient. Conflict preemption exists where compliance

3   with both federal and state regulations is impossible, or where state law stands as an obstacle to

4   the accomplishment and execution of the full purposes and objectives of Congress. *Gade*,

5   505 U.S. at 98. "A holding of federal exclusion of state law is inescapable and requires no

6   inquiry into congressional design where compliance with both federal and state regulation is a

7   physical impossibility for one engaged in interstate commerce." *Fla. Lime & Avocado Growers,*

8   *Inc. v. Paul*, 373 U.S. 132, 142-43 (1963).

9   Plaintiff's application of the CIPA to prevent ECS Providers from scanning, processing,

10   or analyzing emails (FAC ¶¶ 34, 66); or recording or copying emails (*id.* ¶¶ 34, 69) without the

11   consent of the sender conflicts with ECPA and would make it impossible for email providers to

12   serve their users.[5] An ECS Provider must review emails, including their contents, to properly

13   route emails, and perform tasks such as sorting emails in user created email folders. While

14   Plaintiff states that Yahoo! is involved in "creeping and peeping," the alleged conduct <u>actually</u>

15   <u>described </u>is "scanning" emails and "identify[ing]" "keywords" or "patterns" in emails. (*Id.*

16   ¶¶ 31-36.) Under Plaintiff's construction of the CIPA, automatically determining whether an

17   email should be routed to an inbox folder for e-receipts and order confirmations, or for high

18   priority emails, for example, would be a crime.

19   Further, Yahoo! could not comply with both ECPA and the CIPA under Plaintiff's

20   interpretation. Under the CIPA, it is illegal to "record" a "confidential communication" by means

21   of any "electronic . . . recording device" without the consent of both parties. Cal. Penal Code

22   § 632. But providers must necessarily record communications in order to make them accessible

23   to users. Congress included provisions in the SCA that recognize this fact by permitting and

24   regulating the recording and storage of electronic communications (18 U.S.C. §§ 2702-03), as

25   well as including provisions which *compel* service providers to create copies of electronic

26

27   [5] Plaintiff's allegations, taken at face value, would mean an email recipient commits a crime
     under the CIPA if he asks his ECS Provider to pre-sort his email into folders if he does not first
28   obtain the sender's consent to do so.

1 communications (18 U.S.C. § 2704). *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir.

2 2004) (the SCA covers email messages stored on an ISP's server pending delivery to the

3 recipient). If § 632 were thus interpreted to prohibit providers from "recording" and storing

4 emails on their servers, ECS Providers would be subject to conflicting federal and state

5 regulation, rendering it impossible for ECS Providers to provide email services to their

6 subscribers nationwide. Indeed, this is why under federal law, the Ninth Circuit has found that

7 the provisions dealing with communications in electronic storage under 18 U.S.C. § 2701, and not

8 the provisions dealing with intercepts under 18 U.S.C. § 2511, come into play when analyzing

9 access to communications stored on providers' systems. *Konop*, 302 F.3d at 878-80.

10 Moreover, the CIPA would make it impossible to accomplish the full purposes and

11 objectives of Congress as set forth in ECPA. Congress passed ECPA with the knowledge and

12 expectation that providers of electronic mail would need to "create electronic copies of private

13 correspondence for later reference," monitor "a stream of transmissions in order to properly route,

14 terminate, and otherwise manage the individual messages they contain," and "intercept, disclose

15 or use customer communications" in the normal course of business as a "necessary incident to the

16 rendition of the service or to the protection of the rights or property of the provider." (RJN Ex. A

17 at 3, 20.)

18 It was Congress's goal to protect the privacy interests of the users of electronic

19 communications, while also fostering the growth of electronic communication services, and

20 providing a mechanism for law enforcement to gain access to records of electronic

21 communications when necessary. 18 U.S.C. §§ 2701 *et seq.* If CIPA applies to the recording or

22 monitoring of emails on Yahoo!'s servers—<u>conduct that is inherent in providing email service</u>—

23 then Yahoo! would not be able to function as a service provider, much less comply with its

24 preservation obligations under ECPA. *See* 18 U.S.C. §§ 2703-04. While the California

25 legislature has the authority to create laws aimed at protecting privacy by prohibiting certain

26 forms of surveillance, California cannot pursue this goal in a manner that conflicts with

27 Congress's regulatory scheme. *Gade*, 505 U.S. at 103-04 (state could pursue the goal of worker

28 safety, but was restricted in the way that it could do so by federal law). This is true even when a

1   state's regulations are intended to provide greater protections to citizens than federal law might.

2   *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 874-75 (2000) (state law that was designed to

3   create greater driver safety than the "minimum standard" set forth by Congress was preempted

4   because Congress had determined the manner in which it sought to achieve its objectives). If

5   Plaintiff's CIPA claim is allowed to proceed, it will stifle the ability of providers to offer

6   electronic communications services. Plaintiff's CIPA claim should therefore be dismissed.

7   **B.   The CIPA as Applied by Plaintiff Violates the Dormant Commerce Clause.**

8   Plaintiff's attempt to regulate email communication services beyond California's borders

9   through the CIPA violates the Commerce Clause. The Commerce Clause grants Congress the

10 power to regulate interstate commerce. U.S. Const. art. I, § 8, cl. 3. "[T]his affirmative grant of

11 authority to Congress also encompasses an implicit or 'dormant' limitation on the authority of the

12 States to enact legislation affecting interstate commerce." *Healy v. Beer Inst.*, 491 U.S. 324, 326

13 n.1 (1989). The Dormant Commerce Clause applies when an activity "has a substantial effect on

14 interstate commerce such that Congress could regulate the activity." *Conservation Force, Inc. v.*

15 *Manning*, 301 F.3d 985, 993 (9th Cir. 2002) (quotations and citation omitted).[6]

16   If a state statute directly regulates interstate commerce, it is per se invalid. *See Nat'l*

17 *Collegiate Athletic Ass'n v. Miller*, 10 F.3d 633, 638 (9th Cir. 1993). Direct regulation occurs

18 where a state statute controls "commerce that takes place wholly outside of the State's borders,

19 whether or not the commerce has effects within the State," and is invalid "regardless of whether

20 the statute's extraterritorial reach was intended by the legislature." *Healy*, 491 U.S. at 336. The

21 "practical effect" of a challenged statute is "the critical inquiry" in determining whether that

22 statute constitutes direct regulation. *Id.* The "practical effect . . . must be evaluated not only by

23 considering the consequences of the statute itself, but also by considering how the challenged

24 statute may interact with the legitimate regulatory regimes of other States." *Id.*

25   The CIPA, as applied by Plaintiff, directly regulates interstate commerce because it would

26

27 [6] As set forth above, through ECPA, Congress has already regulated ECS Providers' provision of
    electronic communication services. Further, "[t]he internet [is] an instrumentality of interstate
28 commerce." *United States v. Faris*, 583 F.3d 756, 759 (11th Cir. 2009).

1   govern Yahoo!'s handling of email communications occurring wholly outside the boundaries of

2   California. Plaintiff alleges that he is a resident of Alabama and likewise that every member of

3   the putative class resides <u>outside</u> of California. (FAC ¶¶ 1-2.) Plaintiff seeks recovery based on

4   Yahoo!'s alleged handling of emails that he and every other putative class member sent <u>outside</u> of

5   California to Yahoo! email subscribers <u>outside</u> of California. There is no allegation in the

6   Complaint that the Yahoo! subscribers to whom Plaintiff sent his emails were California

7   residents. Rather, Plaintiff's claim extends to emails sent from Alabama <u>to any state in the union</u>

8   and would directly regulate Yahoo!'s handling of those emails in other states <u>under California</u>

9   <u>law</u>. That is impermissible nationwide regulation. *Healy*, 491 U.S. at 336 ("[A] statute that

10   directly controls commerce occurring wholly outside the boundaries of a State exceeds the

11   inherent limits of the enacting State's authority and is invalid . . . ."). Indeed, Plaintiff's counsel

12   has also filed suit against Yahoo! on behalf of a member of the putative class <u>under Arkansas law</u>

13   based on the same type of conduct alleged here—demonstrating that California law need not and

14   should not be applied outside of the boundaries of the State. *See Sheppard v. Google, Inc. et al.*,

15   Case No. 12-civ-4022 SOH (W.D. Ark) (brought on behalf of an alleged Arkansas resident).

16   Moreover, the practical effect of Plaintiff's attempt to apply the CIPA to email

17   communications outside of California would be to impose an inconsistent regulatory regime on

18   email service providers <u>in other states</u>. "[T]he Commerce Clause protects against inconsistent

19   legislation arising from the projection of one state regulatory regime into the jurisdiction of

20   another state." *Healy*, 491 U.S. at 336-37. If non-California residents who send emails to people

21   outside of California could invoke the CIPA, then ECS Providers would have to follow California

22   law throughout the country. *See Nat'l Collegiate Athletic Ass'n*, 10 F.3d at 639 ("The practical

23   requirement that the NCAA would have to use the [Nevada] Statute in enforcement proceedings

24   in every state in the union runs afoul of the Commerce Clause . . . ."). California's law would

25   effectively trump the law of other states, including Alabama (where Plaintiff resides), that do not

26   require the consent of all parties before a communication may be recorded or reviewed. Ala.

27   Code § 13A-11-30(1). Further, in the Ninth Circuit, a "practical effect" analysis considers

28   whether "conflicting, legitimate legislation is already in place or . . . the threat of such legislation

DEFENDANT YAHOO! INC.'S NOTICE OF MOTION AND MOTION TO DISMISS OR STRIKE; MPA IN SUPPORT THEREOF 14
CASE NO. CV12- 03414 PSG LHK
sf-3206847

1   is both actual and imminent." *S.D. Myers, Inc. v. City & Cnty. of San Francisco*, 253 F.3d 461,

2   469 (9th Cir. 2001). Alabama has already promulgated legislation that is in conflict with the

3   CIPA (as have many other states). [7] The CIPA should not be interpreted to create "the kind of

4   competing and interlocking local economic regulation that the Commerce Clause was meant to

5   preclude." *Healy*, 491 U.S. at 337.

6   **C.   The CIPA Cannot Be Applied to Conduct Occurring Wholly Outside of
              California.**

7   Plaintiff's CIPA claim must be dismissed for the additional reason that the claim as pled

8   inherently applies to email communications occurring outside of the State, in violation of the Due

9   Process and Full Faith and Credit Clauses of the United States Constitution and California's own

10   presumption against extraterritorial application of its laws. Plaintiff alleges that he is an Alabama

11   resident and that he seeks to represent a putative class of individuals who reside outside of

12   California. (FAC ¶¶ 1-2.) He does not contend that he has sent emails to any Yahoo! subscribers

13   that reside in California, nor does he allege that Yahoo! otherwise sent his emails to California

14   prior to delivery for purposes of conducting the purported interception and recording that is the

15   subject of the Complaint. This case is thus unlike any others in which courts have applied the

16   CIPA. *See, e.g.*, *NebuAd*, 804 F. Supp. 2d at 1022 (out-of-state resident had statutory standing to

17   sue under the CIPA where it was alleged that web browsing history was sent to and from

18   California); *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95 (2006) (application of

19   California law would not violate due process where complaint was based upon the recording of

20   telephone calls of <u>California</u> clients, while the clients were <u>in California</u>). Here, in contrast,

21   Plaintiff seeks relief under the CIPA for activities wholly outside of California.

22   The Due Process Clause and the Full Faith and Credit Clause of the United States

23

24   ─────────────────────

25   [7] *See., e.g.*, Ala. Code § 13A-11-30(1); Alaska Stat. §§ 42.40.300(a) & 42.20.310(a)(1); Ark.
     Code Ann. § 5-80-120(a); D.C. Code Ann. § 23-542(b)(3); Minn. Stat. Ann. § 626A.D2 subd.
26   2(d); Miss. Code Ann. § 41-29-531(e); Mo. Ann. Stat. § 542.402(2)(3)(Supp.); N.J. Rev. Stat.
     § 2A:156A-4(d); N.C. Gen. Stat. § 15A-287(a); N.D. Cent. Code § 12.1-15-02(3)(c); Ohio rev.
27   Code Ann. § 2933.52(B)(4); Okla. Stat. Ann. Tit. 13, § 176.4(5); R.I. Gen. Laws § 11-35-
     21(c)(3); Tenn. Code Ann. § 39-13-601(b)(5); Utah Code Ann. §§ 76-9-401(2), 76-9-403(1)(a), &
28   77-23a-4(7)(b); W. Va. Code § 62-1D-3(c); Wis. Stat. Ann. §§ 968.31(c) & 885.365(1); Wyo.
     Stat. § 7-3-602(b)(iv).

1   Constitution preclude application of CIPA to the conduct alleged here. A state must have a

2   "significant contact or significant aggregation of contacts to the claims asserted by each member

3   of the plaintiff class, contacts creating state interests, in order to ensure that the choice of [that

4   state's] law is not arbitrary or unfair." *Shutts*, 472 U.S. at 821-22 (quotations and citation

5   omitted). In *Shutts*, the Supreme Court considered the claims of a nationwide class of plaintiffs

6   who brought suit in Kansas state court against Phillips Petroleum, which owned property and

7   conducted substantial business in Kansas. Plaintiffs sued to recover interest on allegedly delayed

8   royalty payments on oil and gas leases, the majority of which related to oil and gas deposits

9   outside of Kansas. The Kansas courts had applied Kansas law notwithstanding that over 99% of

10   the gas leases and some 97% of the putative class members had no apparent connection to the

11   State of Kansas except for the lawsuit. *See id.* at 814-15. The Supreme Court held that Kansas

12   could not constitutionally apply its own law to the claims of the entire class under the Due

13   Process and Full Faith and Credit Clauses of the Constitution. Because there was a material

14   conflict between the substantive law of Kansas and that of Texas and Oklahoma (the other

15   possible sources of law), the due process rights of the defendant were violated by imposing

16   Kansas law upon the defendant. *Shutts* thus establishes constitutional limitations on the power of

17   a state to apply its law to conduct that <u>occurs beyond its borders</u>.

18   The Supreme Court reiterated these same concerns in *State Farm Mutual Automobile*

19   *Insurance Co. v. Campbell*, 538 U.S. 408, 421-22 (2003). There, the Court invalidated the Utah

20   Supreme Court's imposition of a $145 million punitive damages judgment, in part because the

21   jury had relied on the defendant's out-of-state conduct when awarding punitive damages. The

22   Court observed that states "cannot punish . . . conduct that may have been lawful where it

23   occurred." 538 U.S. at 421-22. *State Farm* confirms the presumption, reflected in *Shutts*, that

24   states cannot apply their law to conduct and transactions that occur and would be lawful outside

25   their borders.

26   Yet Plaintiff attempts to do just that. The putative class consists of persons residing

27   outside of California who are sending emails outside of California to Yahoo! email subscribers.

28   The alleged harm is Yahoo!'s interception, and recording of those emails prior to delivery without

the class members' consent. Putting to one side that the alleged conduct is legal under federal

law (*see supra* Parts I.A, I.B), it is also lawful in many (if not all) states in which putative class

members reside and are sending emails, including in those 38 states that require only one-party

consent.[8] California law cannot constitutionally be applied under these circumstances. *See BMW*

of N. Am. v. Gore, 517 U.S. 559, 570-72 (1996) ("[A] State may not impose economic sanctions

on violators of its laws with the intent of changing the tortfeasors' lawful conduct in other

States."); *compare Kearney*, 39 Cal. 4th at 104 ("This is not a case in which California would be

applying [the CIPA] in order to alter a defendant's conduct in another state *vis-à-vis another*

state's residents.") (emphasis added).

Moreover, such extraterritorial application of the CIPA would contravene California's

own presumption against the extraterritorial application of its criminal laws. *See Gentges v.*

Trend Micro Inc., No. C 11-55574 SBA, 2012 U.S. Dist. LEXIS 94714, at *16 (N.D. Cal. July 9,

2012) ("California courts have long acknowledged a general presumption against the

extraterritorial application of state laws."). The California Supreme Court recently confirmed this

well-established presumption: "However far the Legislature's power may theoretically extend,

we presume the Legislature did not intend a statute to be operative, with respect to occurrences

outside the state, . . . unless such intention is clearly expressed or reasonably to be inferred from

the language of the act or from its purpose, subject matter or history." *Sullivan*, 51 Cal. 4th at

1207 (quotations and citation omitted). No such contrary intention exists with respect to the

CIPA.[9] The CIPA states that it is intended to protect the privacy of "the people of this state"

(Cal. Penal Code § 630), and prohibits the interception of transmissions that are sent from, to, or

---

[8] *See* statutes cited *supra*, note 7. As alleged in Plaintiff's original Complaint, not only did
Yahoo! obtain consent from its email users, but Plaintiff himself has continued to send emails
with knowledge of the alleged scanning, thereby impliedly consenting. It thus cannot plausibly
be concluded that no parties to any of the emails sent by Plaintiff and the putative class gave their
consent to have their emails scanned. *See* discussion *supra* at 4:21-5:19 and law cited in support
thereof.

[9] *NebuAd* does not state otherwise. *NebuAd*, 804 F. Supp. 2d at 1026. There, the court
considered only whether an out-of-state plaintiff had statutory standing to sue under the CIPA
given CIPA's express language that its purpose is to protect "the people of this state." The court
expressly did not consider application of the presumption of extraterritoriality given the
allegations that the complained of conduct took place in the state (unlike here). *Id.* at 1027 n.3.

1   within "this state" (Cal. Penal Code § 631).

2   In *Sullivan*, the California Supreme Court held that the presumption against extraterritorial

3   application applied even where an alleged unlawful practice was conceived and implemented by a

4   California defendant from its corporate headquarters in California. 51 Cal. 4th at 1208. The

5   court held that, absent an allegation that the violation of California law occurred in California,

6   California law could not apply. *Id.* Such an allegation is similarly absent here. Plaintiff merely

7   alleges that he and all members of the putative class live outside of California and have sent

8   emails to Yahoo! subscribers, and that the alleged "acts [of interception] in violation of CIPA

9   resulted from business decisions, practices and operating policies that were developed,

10   implemented, and utilized in the State of California." (FAC ¶ 15.) Such allegations are

11   inadequate under *Sullivan* to overcome the presumption against extraterritoriality.

12   **D.   Plaintiff Cannot State a Claim Under the CIPA for Pre-Delivery Access of
             Email by an Email Service Provider.**
13

14   Even if ECPA did not present a bar to Plaintiffs' application of the CIPA and there were

15   no constitutional, due process or exterritorial concerns, Plaintiff's allegations are inadequate to

16   state a claim under the CIPA.

17   As a threshold issue, Plaintiff's claims should be dismissed because the CIPA does not

18   apply to email communication services. By its plain terms, § 632 prohibits "eavesdropping" on a

19   "confidential communication" without the consent of all parties "by means of any electronic

20   amplifying or recording device." Cal. Penal Code § 632. Section 631 prohibits any "tap[ping]"

21   or "unauthorized connection" "with any telegraph or telephone wire, line, cable or instrument,

22   including the wire, line, cable, or instrument of any internal telephonic communication system."

23   Cal. Penal Code § 631(a). It also prohibits attempting to read the contents of a message

24   transmitted over a "wire, line, or cable." Nothing in either provision suggests that it applies to a

25   provider's access to email communications stored by the provider, like Yahoo!, prior to the

26   delivery of email to the recipient. Instead, it is clear from the plain language that the legislature

27   intended to restrict the scope of § 632 to eavesdropping on sound-based communications that can

28   be amplified or recorded, and for § 631 to be restricted to communications carried over a

DEFENDANT YAHOO! INC.'S NOTICE OF MOTION AND MOTION TO DISMISS OR STRIKE; MPA IN SUPPORT THEREOF 18
CASE NO. CV12- 03414 PSG LHK
sf-3206847

telegraph or telephone wire, line, cable or instrument. Emails are neither of these types of communications.[10] This Court should accordingly not extend the CIPA where the California legislature has not, particularly when doing so would drastically expand the statute's criminal application.[11] *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (under the rule of lenity, criminal statutes imposing penalties must be strictly construed in favor of the defendant even when applied in a civil case); *see also Tos v. Mayfair Packing Co.*, 160 Cal. App. 3d 67, 80 (1984) ("When a statute is penal, principles governing construction of penal statutes apply even when the underlying action is civil in nature.").

Under federal law, the Ninth Circuit has already considered whether the definition of "intercept" applies to access to communications in electronic storage with a service provider, and has rejected the application of "intercept" law to such communications. In *Konop*, 302 F.3d at 878-80, the Ninth Circuit endorsed the Fifth Circuit's prior view, that email stored on a provider's system could not be "intercepted" prior to its delivery to the intended recipients. *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994). The court's decision relied on the understanding that interception had to occur "contemporaneously" with transmission, and that the definition of "electronic communications" in the statute was narrower than the definition of "wire communications." Here, the situation is even starker. The CIPA does not by its terms even apply to electronic communications. Applying traditional eavesdropping or interception law to emails, that are by definition stored on Yahoo!'s servers before Yahoo! acts on them, would represent an unprecedented expansion of the CIPA.

1.   Plaintiff Fails to Allege a Violation of Section 632.

Even if the CIPA were to cover email communications, Plaintiff fails to allege facts

---

[10] Unlike the federal Wiretap Act, which was amended per ECPA to include electronic communications, the CIPA has not been amended to cover email communications. In contrast, the California legislature <u>has</u> amended other sections of the California Penal Code to distinguish between "wire communications" and "electronic communications." Cal. Penal Code § 629.51(a). It is thus clear that § 631 simply does not apply to email communications.   Plaintiff's conclusory assertion that "the e-mails are passing over any wire, line, or cable" does not establish otherwise. (FAC ¶ 67.)

[11] No court has expressly considered and determined that the CIPA applies to ECS Providers' provision of email services.

1 sufficient to demonstrate a violation of § 632. That provision applies only to "confidential"

2 communications. Cal. Penal Code § 632(c). Plaintiff, however, merely asserts the legal

3 conclusion that "[t]he content and meaning of the e-mails which Plaintiff and Class Members

4 send to Yahoo! Mail users is private and confidential among those persons in the destination

5 address fields." (FAC ¶ 42.) The Court need not accept as true such bare legal conclusions. *See*

6 *Iqbal*, 556 U.S. at 678.

7   What is missing from the Complaint are any facts suggesting that the "circumstances"

8 under which Plaintiff sent his emails "reasonably indicate" that he "desire[d]" those emails "to be

9 confined to the parties thereto." Cal. Penal Code § 632(c). Under the CIPA, not all

10 communications are presumptively confidential. *See id.* Moreover, email is inherently a

11 "circumstance in which the parties to the communication may reasonably expect that the

12 communication may be overheard or recorded." *Id.* By its very nature, "in order for e-mail to be

13 useful it must be recorded by the receiving computer." *State v. Townsend*, 57 P.3d 255, 260

14 (Wash. 2002). It also must be recorded by an ECS Providers' servers in order for the recipient to

15 gain access to it. *See In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001);

16 *Theofel*, 359 F.3d at 1075. Further, emails by their very nature must be scanned by ECS

17 Providers to determine who the recipient is and to route the email to that recipient. It is therefore

18 not objectively reasonable for Plaintiff to believe that emails he sends to Yahoo! subscribers are

19 "confidential."

20   Plaintiff also fails to allege sufficient facts demonstrating that his emails were intercepted,

21 scanned, or recorded without his consent. For instance, Plaintiff does not allege whether his own

22 service provider requires him to consent to some or all of the same type of alleged review and

23 recording that is the subject of the Complaint, as other providers commonly do. Nor does

24 Plaintiff allege facts demonstrating that he did not send emails to Yahoo! subscribers with the

25 specific knowledge that nearly all Providers take some pre-delivery action on emails, whether

26 honoring the recipients' requests for email-forwarding, auto-response or email sorting of their

27 inbox based on message contents. Moreover, in his prior complaint, Plaintiff alleged that he

28 continues to send emails to Yahoo! subscribers even though he knows that the emails will be

1 reviewed by Yahoo!, thereby implicitly giving his consent to that review. (Original Compl. ¶¶ 5,

2 11.)

3   Further, courts have found that all senders of email implicitly consent to the recording of

4 the message in the same way that a person who leaves a voicemail consents to its recording. *See,*

5 *e.g.*, *Townsend*, 57 P.3d at 260. For instance, in *Townsend*, the court determined that users of

6 email "had to understand that computers are, among other things, a message recording device"

7 and that therefore email users are "properly deemed to have consented to the recording of those

8 messages." *Id.*; *see also State v. Lott*, 879 A.2d 1167, 1170-73 (N.H. 2005) ("Unlike persons

9 using a telephone, however, persons using an instant messaging program are aware that their

10 conversations are being recorded."); *Commonwealth v. Maccini*, 22 Mass. L. Rptr. 393, at *6

11 (Mass. Super. Ct. (Norfolk) 2007) (same). Further, users who transmit messages via a messaging

12 service consent to some review of messages incident to their delivery. *People v. Wilson*, 17 Cal.

13 App. 3d 598, 603 (1971). Thus, not only has Plaintiff failed to allege facts demonstrating a

14 violation of § 632, but it appears that he could not do so through further amendment given the

15 very nature of email communications.

16   **2.   Plaintiff Fails to Allege a Violation of Section 631.**

17   As set forth above, section 631 prohibits wiretapping or other unauthorized access to a

18 telegraph or telephone wire, line, or cable. Absent from the Complaint is any such allegation, nor

19 could there be one given that Plaintiff has put email, and not interception of a telegraph or

20 telephone wire, line or cable, at issue. But even if § 631 applied to electronic communications

21 transmitted over the internet, there is no allegation of unauthorized access to those

22 communications—indeed, Yahoo! owned and was authorized to access its own servers used to

23 send and receive email. *See*, *e.g.*, 18 U.S.C. § 2701(c)(1) (providing that email providers may

24 access the facilities through which they provide communications services). In fact, courts have

25 frequently relied on the SCA to dismiss claims against ECS Providers based on alleged access to

26 or searching of communications stored on their own networks. *See, e.g., Buza v. Yahoo!, Inc.*,

27 No. C 11-4422 RS, 2011 U.S. Dist. LEXIS 122806, at *1 (N.D. Cal. Oct, 24, 2011) (dismissing

28 claims based on alleged unlawful access to stored emails by an ECS Provider); *Fraser v.*

Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003) (ECS Providers may not be held liable for searching stored communications on their own systems); *Reichert v. Elizabethtown College*, No. 10-2248, 2011 U.S. Dist. LEXIS 86837 (E.D. Pa. Aug. 5, 2011) (same).

Further, Plaintiff's attempt to allege a violation of § 631 based on a contention that Yahoo! has "read[], [or] attempt[ed] to read or [to] learn[] the contents or meaning" of any message, report, or communication while it is in transit "over any wire, line, or cable," fares no better. *See* Cal. Penal Code § 631; (FAC ¶¶ 66-67). Though the FAC alleges that Yahoo! engages in "creeping and peeping," the few allegations that actually describe Yahoo!'s conduct demonstrate that what in fact is at issue are automated processes that scan emails sent to Yahoo! subscribers in order to provide services to those subscribers. (FAC ¶ 34.) This sort of review of electronic communications is permitted under federal law. It is also necessary for the delivery of the email, and to provide services for the recipient.[12]

Likewise, all emails *must* be recorded before they are delivered—otherwise the recipient cannot access them. *See In re Doubleclick*, 154 F. Supp. 2d at 511-12 ("[E]lectronic storage" refers to "communications temporarily stored by electronic communications services incident to their transmission–for example, when an email service stores a message until the addressee downloads it."); *see also Theofel*, 359 F.3d at 1075 (observing that an "obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event the user needs to download it again"). Plaintiff thus merely alleges that Yahoo! automatically processed his emails before delivery to the recipients. There is no reason to believe that the California legislature, in 1967, intended to prevent this type of conduct when it enacted the CIPA.[13]

---

[12] Even Plaintiff recognizes that applying the plain text of the CIPA to all email scanning would create absurd results. Tellingly, Plaintiff concedes that some scanning, such as the "automated scanning of e-mail for spam and virus protection," could not violate the CIPA (FAC ¶ 30); but fails to explain what type of scanning <u>could</u> violate the CIPA under his theory, or why some scanning would be legal while other scanning would be illegal.

[13] Indeed, in 1986, when ECPA was enacted, Congress recognized that unlike voice communications, electronic communications require monitoring; and that this monitoring does not involve humans listening in on conversations. (RJN Ex. A at 20.)

1   **II.   PLAINTIFF'S CLASS ACTION ALLEGATIONS MUST BE STRICKEN
2   PURSUANT TO RULE 12(F).**

3   Pursuant to Rule 12(f), the Court "has authority to strike class allegations prior to

4   discovery if the complaint demonstrates that a class action cannot be maintained." *Tietsworth v.*

5   *Sears, Roebuck & Co.*, 720 F. Supp. 2d 1123, 1146 (N.D. Cal. 2010). The class as pled fails to

6   meet the requirements of Rule 23. Rule 23(a) requires a showing that the claim of each putative

7   class member depends upon a "common contention" of "such a nature that it is capable of

8   classwide resolution—which means that determination of its truth or falsity will resolve an issue

9   that is central to the validity of each one of the claims in one stroke." *Wal-Mart Stores, Inc. v.*

10   *Dukes*, __ U.S. __, 131 S. Ct. 2541, 2545 (2011). Rule 23(b)(3) requires a showing that questions

11   of law or fact common to class members predominate over any questions affecting only

12   individual members. *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589 (9th Cir. 2011). The

13   putative class satisfies neither requirement.

14   **A.   Plaintiff Cannot Show There Is a Common Factual Issue That Is Central to
               Each Class Member's Claim, Much Less That Factual Issues Predominate.**
15

16   The class as pled could not be certified because there are numerous material, individual

17   issues of fact that will need to be adjudicated in order to resolve any individual class member's

18   claim. For instance, to show that an email was "confidential," as required under § 632, each

19   individual class member must show that the circumstances under which he or she sent the email

20   "reasonably indicate" that the class member intended the email to be confidential and did not

21   reasonably expect that the email would be shared or recorded. Cal. Penal Code § 632. To the

22   extent that it is objectively reasonable for anyone to believe email is confidential given the nature

23   of that medium of communication, any such determination of each class member's state of mind

24   and the particular circumstances under which he or she sent the email, including the content of the

25   email itself, would necessarily be highly individualized. For instance, some putative class

26   members may have sent an email to a Yahoo! subscriber with the intent, or even the request, that

27   the email be shared, published or made publicly available. Such emails clearly are not

28   "confidential" under the CIPA. *See* Cal. Penal Code § 632(c) (The term "confidential

communication" does not include those where the party did not desire the communication "to be confined to the parties thereto.").

Similarly, if senders of email do not necessarily impliedly consent to having their emails reviewed and recorded (*see supra* Part I.D.1), then the issue of implied consent would at best be a highly individualized determination. That determination would require an inquiry into facts, unique to each putative class member, about his or her knowledge that ECS Providers scan emails; whether he or she had given consent to his or her own Provider to have emails scanned and thus understood that it is a common practice; whether the class member knew that emails are "intercepted" and "recorded" by ECS Providers in order to deliver emails to their subscribers; and a host of other related factual issues bearing on each class member's knowledge and consent.

As a result of these highly individualized factual issues, Plaintiff cannot show a single common fact that will resolve "in one stroke" an issue that is central to the validity of each class member's claim. *Wal-Mart*, 131 S. Ct. at 2545. For the same reason, Plaintiff also cannot show that common factual issues predominate over questions affecting only individual class members. *See Murray v. Fin. Visions, Inc.*, No. CV-07-2578-PHX-FJM, 2008 U.S. Dist. LEXIS 93419, at *12-15 (D. Ariz. Nov. 6, 2008) (finding class certification inappropriate in a suit brought under ECPA and state privacy laws, because determining whether implied or express consent was present, whether each class member had a reasonable expectation of privacy, and whether each disclosed email was confidential required an individualized inquiry).

B. Common Questions of Law Do Not Predominate.

Plaintiff seeks certification of a nationwide class of <u>non-California residents</u> who are not Yahoo! subscribers and who sent emails to individual Yahoo! subscribers. Plaintiff cannot show that common questions of law will predominate for each putative class member's claim because, as set forth above, the CIPA cannot constitutionally be applied to each class member's claim. *See Shutts*, 472 U.S. at 797 (Constitution imposes limitations on a state to apply its law to conduct that occurs beyond its borders). Nationwide application of the CIPA would also be contrary to

California's choice of law rules, which utilize a governmental interest test.[14] *Mazza*, 666 F.3d at 590. Under that test, courts consider (1) whether the relevant laws of affected states are different, (2) if they are different, whether given the interests of the states in the conduct at issue, there is a true conflict, and (3) if there is a true conflict, which state's interest would be most impaired if its policy were subordinated to the policy of the other state. *Id.*

Here, the laws of the various states in which class members reside differ from the CIPA in key ways, including whether the consent of one party to a communication is a sufficient shield against liability for alleged "wiretapping" or "eavesdropping."[15] Further, as recognized in *Mazza*, every state has a strong interest in having its own laws applied to its residents, as well as making its own determination regarding "the appropriate level of liability for companies conducting business within its territory." *Id.* at 591-92. In contrast, "California's interest in applying its law to residents of foreign states is attenuated." *Id.* at 594. Thus, under California's choice of law test, no single state's law may permissibly be applied to the conduct at issue. The differences between the laws of the many affected states "would cast a long shadow over any common issues of fact [P]laintiff[] might establish." *Pilgrim v. Universal Health Card, LLC*, 660 F.3d 943, 946 (6th Cir. 2011); *see also Sanders*, 672 F. Supp. 2d at 991 (striking class action allegations when individual inquiries would predominate, and "these individual inquiries very likely would be subject to the differing state laws that may or may not apply").

CONCLUSION

For the reasons set forth herein, Yahoo! respectfully requests that its motion to dismiss be granted in its entirety or, alternatively, that the Court strike the class action allegations for failure to satisfy the requirements of Rule 23 of the Federal Rules of Civil Procedure.

---

[14] When a federal court sits in diversity, it must look to the forum state's choice of law rules to determine the controlling substantive law. *See Patton v. Cox*, 276 F.3d 493, 496 (9th Cir. 2002).

[15] *See, e.g.,* statutes cited *supra* note 7.

1   Dated: October 30, 2012   MORRISON & FOERSTER LLP

2

3   By: /s/ Rebekah Kaufman
                                                                 REBEKAH KAUFMAN
4
                                                                 Attorneys for Defendant
5   YAHOO! INC.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28